



USAISEC

*US Army Information Systems Engineering Command
Fort Huachuca, AZ 85613-5300*

4

U.S. ARMY INSTITUTE FOR RESEARCH
IN MANAGEMENT INFORMATION,
COMMUNICATIONS, AND COMPUTER SCIENCES
(AIRMICS)

AD-A217 406

TECHNOLOGY ASSESSMENT OF AUTOMATION SECURITY

(ASQBG-A-89-007)

February, 1989

DTIC
ELECTE
JAN 18 1990
S B D

AIRMICS
115 O'Keefe Building
Georgia Institute of Technology
Atlanta, GA 30332-0800



DISTRIBUTION STATEMENT A

Approved for public release
Distribution Unlimited

90 01 17 026

REPORT DOCUMENTATION PAGE

Form Approved
OMB No 0704-0188
Exp Date Jun 30, 1986

1a. REPORT SECURITY CLASSIFICATION UNCLASSIFIED			1b. RESTRICTIVE MARKINGS NONE		
2a. SECURITY CLASSIFICATION AUTHORITY N/A			3. DISTRIBUTION / AVAILABILITY OF REPORT N/A		
2b. DECLASSIFICATION / DOWNGRADING SCHEDULE N/A					
4. PERFORMING ORGANIZATION REPORT NUMBER(S)			5. MONITORING ORGANIZATION REPORT NUMBER(S) N/A		
6a. NAME OF PERFORMING ORGANIZATION AIRMICS		6b. OFFICE SYMBOL (If applicable) ASQBG-A	7a. NAME OF MONITORING ORGANIZATION N/A		
6c. ADDRESS (City, State, and ZIP Code) 115 O'Keefe Bldg., Georgia Institute of Technology Atlanta, Georgia 30332-0800			7b. ADDRESS (City, State, and ZIP Code) N/A		
8a. NAME OF FUNDING / SPONSORING ORGANIZATION AIRMICS		8b. OFFICE SYMBOL (If applicable) ASQBG-A	9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER		
8c. ADDRESS (City, State, and ZIP Code) 115 O'Keefe Bldg., Georgia Institute of Technology Atlanta, Georgia 30332-0800			10. SOURCE OF FUNDING NUMBERS		
			PROGRAM ELEMENT NO. 62783A	PROJECT NO. DY10	TASK NO. 00-08
			WORK UNIT ACCESSION NO.		
11. TITLE (Include Security Classification) Technology Assessment of Automation Security (UNCLASSIFIED)					
12. PERSONAL AUTHOR(S) Paul T. Hengst					
13a. TYPE OF REPORT		13b. TIME COVERED FROM _____ TO _____		14. DATE OF REPORT (Year, Month, Day) 1989, February	
15. PAGE COUNT 14					
16. SUPPLEMENTARY NOTATION					
17. COSATI CODES			18. SUBJECT TERMS (Continue on reverse if necessary and identify by block number)		
FIELD	GROUP	SUB-GROUP	Security, Automation, and Technology Assessment		
19. ABSTRACT (Continue on reverse if necessary and identify by block number)					
<p>An assessment of current, near-term (1995), and long-term (2010) trends in automation security is given. The five general areas within automation that are addressed are: access, storage methods, anti-viral measures, operation of systems, and accreditation.</p>					
20. DISTRIBUTION / AVAILABILITY OF ABSTRACT <input checked="" type="checkbox"/> UNCLASSIFIED/UNLIMITED <input type="checkbox"/> SAME AS RPT <input type="checkbox"/> DTIC USERS			21. ABSTRACT SECURITY CLASSIFICATION UNCLASSIFIED		
22a. NAME OF RESPONSIBLE INDIVIDUAL Paul T. Hengst			22b. TELEPHONE (Include Area Code) (404) 894-3107		22c. OFFICE SYMBOL ASOBG-A

This research was performed as an in-house project at the Army Institute for Research in Management Information, Communications, and Computer Sciences (AIRMICS), the RDTE organization of the U.S. Army Information Systems Engineering Command (USAISEC). This effort was performed under the AIRMICS Technology Insertion Program to support the U.S. Army Information Systems Command (USAISC) in the development of a report entitled "Long Range Planning Guidance - Objective Configuration." An initial meeting was held in early December in Atlanta to coordinate the task. Twenty-six topics were selected for consideration, with AIRMICS agreeing to conduct technology assessments on fifteen of the topics. Planning Research Corporation (PRC) was assigned responsibility for conducting the remaining assessments and consolidating all the assessments for use in the planning document. In a two-week period, AIRMICS completed the assessments and provided the results to ISC-DCSPLANS and ISEC-SID. This research report is not to be construed as an official Army position, unless so designated by other authorized documents. Material included herein is approved for public release, distribution unlimited. Not protected by copyright laws.

THIS REPORT HAS BEEN REVIEWED AND IS APPROVED



s/ James D. Gantt
 James D. Gantt, Chief
 Management and Information
 Systems Division

s/ John R. Mitchell
 John R. Mitchell
 Director
 AIRMICS

For	
SI	<input checked="" type="checkbox"/>
ed	<input type="checkbox"/>
ion	<input type="checkbox"/>

Distribution/	
Availability Codes	
Dist	Avail and/or Special
A-1	

Automation Security

I. Historical Review

The entire security area is receiving an increasing amount of attention from industry. The Information Systems Security Association has gone from 100 members in 1984 to 1350 today. [1] This increasing attention is also seen in the number of security related projects in the Independent Research and Development (IR&D) program. A part of this increase can be attributed to the attention given this area by government and the press. The Information Security Act of 1987 calls for the protection of unclassified but sensitive data.[2] This is a fundamental switch from when only classified information required protection. This will mean that thousands of information systems within the government that formerly did not require protection will now need some security measures.

However, the requirement for secure systems today outstrips the ability of the technology to provide what is needed. Although envisioned for over a decade, a true multilevel secure system has not been developed at a reasonable cost. A multilevel secure system (MLS) has the ability to store or access data or information of various degrees of security on a single computer. With the increasing number of information systems and the vast number of microcomputers in place, we will be unable to replace all current systems with single classification systems. Therefore, the most cost beneficial method is to develop the operating system and software that is able to support MLS systems.

This technology assessment will examine five general areas within the automation security area. Those five areas are access, storage methods, anti-viral measures, operating systems, and accreditation. Each area will be examined for the current state of the technology, where the technology should be in the 1995 time frame, and an estimate of the technology in the year 2010.

II. Currently Available

Many of the techniques and technologies that support automation security are still in their infancy. As stated above, a number of vendors are working in each area to develop solutions. The competition is keen, because the first vendor with a cost affordable MLS system may be able to set the de facto standard.

A. Access

Future automation security must be able to support the ability to deny access to information and data stored on computers at both the user, services, and network levels. The user level will control the individual's ability to use the machine. Some machines may contain data or information that is not available to all users. The service access control will manage the access to various applications and utilities stored or running on a machine or network. The network requirement includes both LANs and WANs. The increasing number of connected (and distributed) systems will force system designers to plan for others to access the system.

Currently, user access security takes a number of forms, both electronic and physical. However, the most common approach used today is passwords. There are well documented studies of the shortfalls of using passwords. [3] With the increasing computational speed of the computer, soon even the most secure passwords may be discovered in a short period of time. To overcome these shortfalls, considerable efforts are underway with a number of vendors to develop new techniques for providing security. Although still in its infancy as a technology, the use of biometrics is receiving considerable attention. A number of devices that measure a biometric feature of the individual (retinal pattern, thumb or hand print, typing or keystroke dynamics, voice print) and use that information to allow the individual to gain access to the computer or network, are available on a small scale or are being developed. The cost of available methods prevents

their wide use. [4] Another alternative is the use of smart cards that a user inserts into a machine to determine access. Like biometrics, this method is expensive because of the hardware costs. Unlike biometrics, the loss of a card has the same ramifications as giving out your password.

Today the services available to the user are determined by the individual's ability to access a particular machine. If the user can gain access to a machine, then he or she can in most cases use the services and programs on that machine. While on some critical systems there are file locking mechanisms, these same mechanisms are not available on administrative systems or the mechanism is at a very low level. These low level mechanisms include read-only files and passwords to gain access to the service. Most of the service protection today is provided through the machine or user access described above. This is almost always the case on microcomputer systems.

As in the machine access, most networks use passwords or in some cases layers of passwords. These passwords, like their user counterparts, are not a very secure way of protecting the system. There is an additional threat in that the passwords for the entire system are stored in a single password table. Therefore, the malicious user could gain access to the password files, possibly compromising all users and files on the system. With the proliferation of network systems, this becomes an increasing problem. Like the user access, biometrics are being tested for access techniques. However, unlike single user systems, all terminals or stations must have similar security equipment or methods for gaining access. In addition, the storage overhead for large systems is significant.

B. Data and Information Storage Methods

The key to MLS systems is the ability to store, retrieve, and process data of various security levels on a single machine or system. As stated above, there are no true MLS machines that are reasonably available. Honeywell SCOMP has many MLS features but is

not cost effective on a wide scale. There are several storage methods used today that provide a degree of security. However, all of these methods must undergo a degree of change as the Army moves toward more distributed systems.

Current secure systems operate at a single level, i.e. Top Secret, Secret, or Confidential. All data residing on those marked systems may not need to be classified. However, to maintain data integrity the data is protected as if it was classified. This method protects the data but is costly and prevents data sharing.

To overcome some of the weaknesses of the single level systems, guard systems are being employed. An example is the FORSCOM Guard system. [5] The guard system is another secure computer that resides between systems or computers of different classifications. The guard has the function of "checking" to see that only authorized data can be passed from one system to another. As an example, Secret data from one system could not be passed to a system that only handles Confidential data. However, Confidential data could be passed to a system rated at Secret. The guard enforces the policy rules programmed into it. In addition, the guard can also enforce some of the access techniques described above. The problem with guard systems is that another layer of machines and software is required to enforce the security policy, which increases the initial and life cycle costs. The benefit to the guard is that some degree of data sharing is allowed.

At the data element level encryption is a primary method for protecting the data. [6] Encryption algorithms can be employed on micros to mainframes. The encryption algorithms employed may be very sophisticated (DES) or very low level (many of the PC products). The degree of protection provided is directly correlated to the sophistication of the algorithm and consequently the cost. However, encryption does provide a reasonable degree of protection for the cost.

The major problem with encryption today is the number of systems and algorithms employed. The wide variance prevents data sharing between users with different systems. Users wishing to share data that use different algorithms must first decrypt the data, share the data (transmit in the clear, swap unprotected disk, etc.) then encrypt back into the particular system used by each user. There are a number of vendors working in this area. The key to wide-spread data sharing will be the ability to share encryption keys on a reliable basis. [7] Public key encryption was in the vogue just a few years ago and some products did emerge, however there are still problems with this technology. The work GTE is doing on Secure Data Network System (SDNS) will provide a key management alternative.

There are some physical measures that are being developed that also provide a limited degree of protection. Among these are read-only media and removable media. Removable disks cartridges can be removed from the machine and stored in secure areas thereby denying access to other individuals that use that machine or are connected to the network. The removable disks can be anything from a disk pack on a mainframe to a removable hard drive on a micro. The current problem with this technology is that as miniaturization continues, the removable items become smaller and therefore easier to conceal. It is literally possible for the business to "walk out the door" with some of the new removable technologies.

The current state of the technology in this area calls for layers and multiple techniques to be employed. An example may be an encryption scheme employed on a removable disk. The greater number of layers, the greater degree of security. However, each layer brings with it a certain amount of overhead that must be taken into account when determining system performance.

C. Anti-Viral Measures

The threat of a computer virus (or worm, trojan horse, trapdoor, etc.) is one of the leading concerns today. These attacks on the system can be perpetrated from personnel within the organization or from an outside intruder. [8] The increase in connectivity has increased the possibility of a single virus shutting down or destroying data over a number of interconnected networks.

The current measures taken to discover or prevent viruses are not very sophisticated and rely in many cases on common sense on the part of the user and administrator. These measures include loading only trusted software, testing software off-line before installing on on-line systems, employing call-back procedures on modems and other outside links, and routinely checking audit trails created by the machine or network. There are a number of automated programs available at a reasonable price to assist the user. [9] However, most of these products are PC- or workstation-based. Automated measures to prevent viruses on mainframes or networks are not in place on a wide scale. Some systems, like NASA's, are properly safeguarded; however most military networks are not protected to the degree required.

D. Secure Operating Systems

The Honeywell SCOMP is the only A1 approved secure operating system available in today's market place. [10] The operating system is being used in several applications in place today. However, there has not been widespread use of the operating system because it is tied to a specific family of platforms only available from Honeywell. Until this is remedied the system will remain a hardware-dependent system.

There are a number of vendors working on secure UNIX based operating systems. [11] Most of these operating systems are not aimed for the A1 market at this time. However, the systems being developed are not platform-bound. This will make them

useful over a range of systems. The only problem will be if multiple systems are deployed, there may be some problems in transferring data between different operating systems.

In addition to the industry efforts, the Army (CECOM) in conjunction with the National Computer Security Center has been working on a secure operating system (ASOS). [12] ASOS is aimed at A1 for multilevel systems and C2 for real-time systems. The system is programmed in Ada and targeted for the 68020 family of computers. There is currently no date for the full implementation of the ASOS.

E. Accreditation

A major hurdle in the acceptance of any part of a secure system is the accreditation. This is true for both hardware and software. Currently, there are a number of players that are involved in the accreditation process. This includes NSA, NCSC, DCA and others. Currently the "Rainbow" series of reference materials published by NCSC is used to determine the degree of security required and the ability of the hardware or software to meet that requirement. [13]

There are some automated tools today that can assist the developer in the acceptance test. [14] However, these tools are not wide spread or can only be used on a limited bases. Consequently, there is a long time lag, two to three years on average, from the time a product is submitted for accreditation until the final accreditation is given. The only method today to speed up this process is on a policy exception basis. [15] Either the policy can be changed, which is unlikely based on recent events, or waivers can be granted. Several vendors and NIST are working on risk assessment models that may produce automated tools to help in the accreditation process.

III. Near Term (1995)

A. Machine and Network Access

Access will still remain the first level of defense against entry into a system or network. The methods to do this will still be password-based. However, biometric measures will continue to be employed as cost-effective devices or imbedded devices become available. There will be layers of security to use a machine, enter a network, and run an application. These layers may start out with the simple and less expensive measures, such as passwords, and end up with more complex measures running on a network server. Access mechanisms will continue to lag behind connections. The requirement for fully connected networks and networks of networks will continue to grow, without a corresponding growth in access techniques. Only new systems will have security built in from the start. Older or mature networks will still have patchwork or add-on access methods.

B. Data and Information Storage Methods

There will not be any major revolutionary changes in data and information storage methods. Encryption algorithms will be more complex and harder to break. There will be an increase in the number of vendors and consequently products.

There will be the beginning of some security standards. These standards will be embedded in other larger standards and protocols suites, such as OSI. [16] Much of the security at this layer will start to become transparent to the user. Encryption algorithms will be automated to change at various time periods, all unknown to the user.

Removable products will be affordable on a wide scale and will see increased use. However, they will not be totally portable to all systems because of the encryption algorithms employed.

C. Anti-Viral Measures

Due to the recent publicity and emphasis in this area, there will be a greater number of automated measures available. The creation of the full time Computer Emergency Response Team will lead to a clearing house for information on virus programs and anti-virus procedures. [17]

By this time, there will be the start of intelligent audit mechanisms. While not fully capable of stopping a virus, these programs will be able to recognize virus attributes and notify systems administrators. To some degree, the programs may be intelligent enough to try to contain the virus by shutting off access to certain parts of the system.

Vaccine-type programs will exist in a number of formats, for large and small systems. However, these will still be fairly straightforward programs requiring overhead that will rob processing power.

The burden to apply safe measures will fall more to the system administrator as more centrally-based servers are employed. A limited number of automated tools will be available to the administrator for the testing of programs prior to installation. Additionally, automated backup and recovery methods will reduce the re-installation time following an attack or suspected attack on the system.

D. Secure Operating Systems

At the lower security levels, B2 and below, there will be several secure operating systems. These operating systems will be built around the UNIX operating systems. These secure operating systems will be used in a number of isolated or "guarded" systems. The operating systems will not be capable of true MLS operation. There will be a move away from proprietary hardware/software systems and more of a general secure operating system capable of running on a variety of hardware platforms.

E. Accreditation

The accreditation process will still remain complicated and policy driven. A1 will still be the target, while some work for systems beyond A1 will start. The current work in risk assessment and threat models will begin to bear fruit by helping designers/engineers to identify their security requirements early in the project. These risk tools will be automated and capable of being used by non-security professionals. [18] There will be an increasing number of automated verification tools, which will aid in the accreditation process.

IV. Long Term (2010)

A. Machine and Network Access

Access methods will be advanced to the point where passwords will be in use on only the smallest and least secure systems. A variety of access control techniques will be in place, to include inexpensive biometric measures. New technologies and advances in distributed systems will help to control access across multiple networks.

MLS data storage methods will decrease some of the access requirements. This will move the emphasis from the network or machine level to the data level. If the data can be protected from misuse, then it does not matter if an unauthorized user has access. However, to insure a greater degree of security, there will still be access control. These controls will become more transparent to the user over time. The transparency will be necessary due to the use of distributed systems. User access profiles will establish the systems/networks and applications/data each user has authority to access at the time of logon.

B. Data and Information Storage Methods

Data and information storage methods will be complex and much different than today's methods. The wide spread use of distributed systems will call for security mecha-

nisms that protect by process and user. There will not be a single lock as used today. This will call for an increased amount of metadata on each piece of data or information. This increased overhead will only be possible with increases in processor speed and storage methods. True MLS machines exist which will reduce the number of single security level systems. Some extremely sensitive systems will still operate in a standalone network mode with sophisticated guards for times when data sharing is required.

C. Anti-Viral Measures

Virus attacks will not be as major a concern as they are today. With the advent of MLS storage and protection at the data element level, the concern to stop attacks will be lessened. However, there will still be security measures attached to the audit trail to track system use. These audit methods will employ both automated intelligence and decision-making capability. The audit programs will be able to identify attacks, stop the attack, determine the source of the attack, and clean up any residuals from the attack. The implementation of these programs will decrease the number of attacks on networks. The major concern at this point will be malicious machine entry. These will be dedicated intelligent machines employing fast multiple parallel processors that have the sole purpose of attempting unauthorized entry. The machines will have the capability to learn based on multiple attacks.

D. Secure Operating Systems

There will be widespread use of secure operating systems. This is because almost all operating systems will have embedded security functions. The operating systems will operate at different security levels. The security level will be determined by the user requirement. The level differentiation will be transparent to the user. The operating systems will be able to run in a variety of environments and hardware platforms.

E. Accreditation

Accreditation will still be a part of any security system. However, the actual process will be made easier, by the use of automated security tools throughout the design to implementation process. Requirements determined early in the design phase by risk and threat assessment tools will be fed in to verification systems for final validation. The verification systems will be complex automated systems capable of testing each of the policy requirements. The system will take advantage of high speed processors and parallelism to reduce the testing time.

For application accreditation, software designers will be able to take advantage of secure software libraries. These libraries will consist of reusable modular code that has previously been validated. This will reduce the time necessary for writing secure applications and speed the time necessary in the accreditation process.

V. References

[1] "Fighting Back at Computer Pranksters" The Atlanta Constitution, 18 November 1988, p. B1.

[2] "Network Security", Federal Computer Week, 17 August 1987, p. 26.

"The Computer Security Act of 1987 - A Focus on How NIST/NSA Will Interact on Policy, Implementation and Technology", Briefing given at the 11th Annual National Computer Security Conference, 18 October 1988, Baltimore, MD.

[3] "A comprehensive Approach to Network Security", Data Communications, April 1985, p. 201.

[4] "Biometrics: Personal Keys to Control Access", Federal Computer Week, 17 October 1988, p. 26.

"Exotic Hardware Boots Security", Digital Review, 12 September 1988, p. 73 - 75

"Voice, finger, and retina scans: Can biometrics secure your shop?", Computer-world, 15 February 1988.

[5] "The Best Available Technologies for Computer Security", IEEE Transactions, July 1983, p. 92.

[6] "Data Encryption Can Protect Transmissions" Government Computer News, 18 December 1987, p. 52.

"How to Find Your Way Through the Encryption Maze", Government Computer News, 29 April 1988, p. 39.

[7] "Protecting Public Keys and Signature Keys", Computer, February 1983, p. 27 - 35.

"Choosing a Key Management Style that Suits the Application", Data Communications, April 1986, p. 149 - 160.

[8] "Computer Security: The Menace is From Inside", The Office, October 1988, p. 45 - 46.

[9] "Micro Security Products", Government Computer News, 7 November 1988, pp. 69 - 73.

"Basics Go a Long Way in Security Products", Government Computer News, 18 December 1987, p. 40.

[10] "SCOMP: A Solution to the Multilevel Security Problem", Computer, July 1983, pp. 26 - 34.

[11] "Secure Unix Aimed at Fed Deals", Computerworld, 7 November 1988, p. 25.

"AT&T Offers Secure Unix Software", Federal Computer Week, 5 December 1988, p. 33.

"Sun's New Unix to be Its Most Tamperproof Yet", PC Week Connectivity, 5 December 1988, p. C/8.

[12] ASOS Briefing Slides - 1986.

[13] Department of Defense Trusted Computer System Evaluation Criteria, DOD 5200.28-STD. December 1985.

[14] "A Gypsy Verifier's Assistant", Proceedings 10th National Computer Security Conference, pp. 183 -192.

"Use of Automated Verification Tools in a Secure Software Development Methodology", Proceedings 11th National Computer Security Conference, pp. 284 -289.

"Static Analysis Tools for Software Security Certification", Proceedings 11th National Computer Security Conference, pp. 290 -297.

[15] "Security Evaluations of Computer Systems", Proceedings 10th National Computer Security, pp. 273 -276.

[16] "DOD Order Secure OSI Network", Federal Computer Week, 21 March 1988, p. 10.

[17] "DOD Creates SWAT Team for Computer Viruses", Management Information Systems Week, 12 December 1988, p. 12.

[18] "NBS Model to Measure Risks to Systems", Federal Computer Week, 29 August 1988, p. 10.

"A Risk Analysis Model for the Military Environment", Proceedings 11th National Computer Security Conference, pp. 43 - 52.

"Knowledge-Based Modeling of System Usage for Risk Management", Proceedings 11th National Computer Security Conference, pp. 53 - 58.